

# SHGetFolderPath

The destination string buffer must be long enough to hold the return file path.

Sean Barnum, Digital, Inc. [vita<sup>1</sup>]

Copyright © 2007 Digital, Inc.

2007-04-16

## Part "Original Digital Coding Rule in XML"

Mime-type: text/xml, size: 5193 bytes

<b>Attack Category</b>	<ul style="list-style-type: none"><li>Path spoofing or confusion problem</li></ul>																						
<b>Vulnerability Category</b>	<ul style="list-style-type: none"><li>Buffer Overflow</li><li>Unconditional</li></ul>																						
<b>Software Context</b>	<ul style="list-style-type: none"><li>Shell Functions</li><li>File Path Management</li></ul>																						
<b>Location</b>	<ul style="list-style-type: none"><li>shlobj.h</li></ul>																						
<b>Description</b>	The destination string buffer for SHGetFolderPath() and similar functions must be long enough to hold the return file path. Otherwise, buffer overflows will occur.																						
<b>APIs</b>	<table border="1"><thead><tr><th>Function Name</th><th>Comments</th></tr></thead><tbody><tr><td>SHGetFolderPath</td><td></td></tr><tr><td>SHGetFolderPathA</td><td></td></tr><tr><td>SHGetFolderPathAndSubDir</td><td></td></tr><tr><td>SHGetFolderPathAndSubDirA</td><td></td></tr><tr><td>SHGetFolderPathAndSubDirW</td><td></td></tr><tr><td>SHGetFolderPathW</td><td></td></tr><tr><td>SHGetSpecialFolderPath</td><td></td></tr><tr><td>SHGetSpecialFolderPathA</td><td></td></tr><tr><td>SHGetSpecialFolderPathW</td><td></td></tr></tbody></table>			Function Name	Comments	SHGetFolderPath		SHGetFolderPathA		SHGetFolderPathAndSubDir		SHGetFolderPathAndSubDirA		SHGetFolderPathAndSubDirW		SHGetFolderPathW		SHGetSpecialFolderPath		SHGetSpecialFolderPathA		SHGetSpecialFolderPathW	
Function Name	Comments																						
SHGetFolderPath																							
SHGetFolderPathA																							
SHGetFolderPathAndSubDir																							
SHGetFolderPathAndSubDirA																							
SHGetFolderPathAndSubDirW																							
SHGetFolderPathW																							
SHGetSpecialFolderPath																							
SHGetSpecialFolderPathA																							
SHGetSpecialFolderPathW																							
<b>Method of Attack</b>	Buffer Overflow																						
<b>Exception Criteria</b>																							
<b>Solutions</b>	<b>Solution Applicability</b>	<b>Solution Description</b>	<b>Solution Efficacy</b>																				
	Whenever one of the indicated functions is used.	The output parameter, pszPath, must be at least MAX_PATH characters (not	Effective.																				

1. [http://buildsecurityin.us-cert.gov/bsi/about\\_us/authors/35-BSI.html](http://buildsecurityin.us-cert.gov/bsi/about_us/authors/35-BSI.html) (Barnum, Sean)

		bytes, in the case of wide characters) in length.
<b>Signature Details</b>		<pre> HRESULT SHGetFolderPath(     HWND hwndOwner,     int nFolder,     HANDLE hToken,     DWORD dwFlags,     LPTSTR pszPath ); HRESULT SHGetFolderPathAndSubDir(     HWND hwnd,     int csidl,     HANDLE hToken,     DWORD dwFlags,     LPCTSTR pszSubDir,     LPTSTR pszPath ); BOOL SHGetSpecialFolderPath(     HWND hwndOwner,     LPTSTR lpszPath,     int nFolder,     BOOL fCreate ); </pre>
<b>Examples of Incorrect Code</b>		<pre> TCHAR szPath[17]; // Buffer not large enough if(FAILED(SHGetFolderPath(NULL, CSIDL_PERSONAL CSIDL_FLAG_CREATE, NULL, 0, szPath))) { /* handle error */ } </pre>
<b>Examples of Corrected Code</b>		<pre> TCHAR szPath[MAX_PATH]; // Buffer correctly sized if(FAILED(SHGetFolderPath(NULL, CSIDL_PERSONAL CSIDL_FLAG_CREATE, NULL, 0, szPath))) { /* handle error */ } </pre>
<b>Source Reference</b>		<ul style="list-style-type: none"> <li>• <a href="http://msdn.microsoft.com/library/default.asp?url=/library/en-us/shellcc/platform/shell/reference/functions/shgetfolderpath.asp">http://msdn.microsoft.com/library/default.asp?url=/library/en-us/shellcc/platform/shell/reference/functions/shgetfolderpath.asp</a><sup>2</sup></li> </ul>
<b>Recommended Resources</b>		<ul style="list-style-type: none"> <li>• <a href="#">MSDN reference for SHGetFolderPath</a><sup>3</sup></li> <li>• <a href="#">MSDN reference for SHGetFolderPathAndSubDir</a><sup>4</sup></li> <li>• <a href="#">MSDN reference for SHGetSpecialFolderPath</a><sup>5</sup></li> </ul>
<b>Discriminant Set</b>	<b>Operating System</b> <b>Languages</b>	<ul style="list-style-type: none"> <li>• Windows</li> <li>• C</li> </ul>

## Cigital, Inc. Copyright

Copyright © Cigital, Inc. 2005-2007. Cigital retains copyrights to this material.

Permission to reproduce this document and to prepare derivative works from this document for internal use is granted, provided the copyright and “No Warranty” statements are included with all reproductions and derivative works.

For information regarding external or commercial use of copyrighted materials owned by Cigital, including information about “Fair Use,” contact Cigital at [copyright@cigital.com](mailto:copyright@cigital.com)<sup>1</sup>.

The Build Security In (BSI) portal is sponsored by the U.S. Department of Homeland Security (DHS), National Cyber Security Division. The Software Engineering Institute (SEI) develops and operates BSI. DHS funding supports the publishing of all site content.

---

1. <mailto:copyright@cigital.com>